Common Policy Change Proposal

Change Number: 2005-03

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Common Certificate Policy

Date: 18 August 2005

Title: Addition of High Assurance Policy to the Common Policy Framework

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Common Policy Framework Version 2.2, 29 March 2005.

Change Advocates Contact Information:

Name: Tim Polk
Organization: NIST
Telephone number: 301-975-3348
E-mail address: tim.polk@nist.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: Agencies with a requirement for high assurance PKI credentials have requested a new Common Policy High Assurance.

Background: This requirement was discussed in the Federal PKI Policy Authority. The FPKI PA directed the CPWG to develop an additional policy in the Common Policy framework that meets all the requirements for the FBCA High Assurance policy.

Issue

Agencies are required to migrate to the Common Policy as directed in OMB 05-05. Currently, agencies that issue high assurance credentials would assert the common hardware OID and an agency specific high assurance policy OID. Such agencies would need to perform compliance audits against both policies. By establishing the Common Policy for High Assurance, agencies can simplify audit process while meeting both OMB's and the agency's requirements.

Specific Changes:

Specific changes are made to the sections 1.2, 3.2.2, 4.4.3.1, 4.5.2, 4.6.2, 6.1.1.1, 6.2.1, 6.2.4.2, and 6.3.2. Insertions are underlined, deletions are in ~~strikethrough~~.

1.2 IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP shall assert at least one of the following OIDs in the certificate policy extension:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users to support digitally signed documents or key management may contain either the id-fpki-common-policy, ~~or~~ id-fpki-common-hardware, or id-fpki-common-High. Certificates issued to devices under this policy include the id-fpki-common-devices.

Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. The id-fpki-common-authentication policy is identical to id-fpki-common-hardware, excepting the key usage constraints as mentioned in Section 7.1.10.

3.2.2 Certificate Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

For policies other than id-fpki-common-High, if it has been less than 6 years since a subscriber was identified as required in Section 3.1, a CA may authenticate an electronic request for a new certificate using the currently valid certificate issued to the subscriber by the CA. Subscribers shall identify themselves for the purpose of re-keying through use of current signature key.

~~CA certificate Re-Key shall follow the same procedures as initial certificate issuance.~~ If more than 6 years have passed since a subscriber's identity was authenticated as specified in Section 3.1, a subscriber certificate re-key shall follow the same procedures as initial certificate issuance.

CA certificate Re-Key and re-key of certificates issued under id-fpki-common-High shall follow the same procedures as initial certificate issuance.

4.4.3.1 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for offline or remote (laptop) operation.

CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

CAs that only issue certificates to CAs and that operate offline must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 24 hours after issuance time (i.e. the *thisUpdate* time). CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 18 hours after issuance time (i.e. the *thisUpdate* time). When a CA certificate or subscriber certificate issued under id-fpki-common-High is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.

4.5.2 Frequency of Processing Data

For CAs that issue certificates under id-fpki-common-High, review of the audit log shall be required at least once every month. ~~Review~~ For CAs that do not issue certificates under id-fpki-common-High, review of the audit log shall be required at least once every two months.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA since the last review shall be examined. This amount will be described in the CPS.

All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

4.6.2 Retention Period for Archive

For CAs that issue certificates under id-fpki-common-High, archive records must be kept for a minimum of 20 years and 6 months without any loss of data.

For CAs that do not issue certificates under id-fpki-common-High, ~~The~~ archive records must be kept for a minimum of 10 years and 6 months without any loss of data.

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 validated cryptographic modules. For CAs that issue certificates under id-fpki-common-High, the module(s) shall meet or exceed Security Level 3. For CAs that do not issue certificates under id-fpki-common-High, the module(s) shall meet or exceed Security Level 2. Multiparty control is required for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [FIPS 140-2]. The PA may determine that other comparable validation, certification, or verification standards are sufficient. The PA will publish these standards. Cryptographic modules shall be validated to a FIPS 140 level identified in this section, or validated, certified, or verified to requirements published by the PA.

CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. RAs~~The CA and RA~~ shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under either the hardware users policy (id-fpki-common-hardware) or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

6.2.4.2 Backup of Subscriber Private Keys

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-High policy may not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert id-fpki-common-High may be backed up or copied, but must be held in the subscriber’s control. Backed up subscriber private keys must be encrypted using a symmetric algorithm of consistent strength or stored in a cryptographic module validated at FIPS 140 Level 2.

6.3.2 Usage Periods for the Public and Private Keys

The usage period for a CA key pair is a maximum of six years. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period. [Practice Note: For example, where subscriber certificates are issued with a three year lifetime, the CA private key may be used to generate certificates for the first half of the usage period (3 years), and the CA public key may be used to validate certificates for the entire usage period.] If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.

Subscriber public keys have a maximum usage period of one half the CA key pair usage period. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

Estimated Cost:

No cost.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Common Policy CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	various throughout 2005
Date Presented to FPKI PA:	September 13, 2005
Date of approval by FPKI PA:	September 13, 2005